We claim:

1. An identification document comprising:

an OVD with embedded machine readable data, the embedded machine readable data encrypted with an encryption key;

a substrate comprising one or more structures carrying data that is associated with the machine readable data embedded in the OVD.

2. The document of claim 1 wherein the OVD comprises at least one of a KINEGRAM® and an embossed hologram, the OVD having an embedded digital watermark.

3. The document of claim 2 wherein the digital watermark carries at least one of an issuer identifier and a machine readable signature related to at least one other element of the identification document.

4. The document of claim 3, wherein the identification document further comprises nanoparticle material having a unique machine readable magnetic signature and wherein the digital watermark carries information relating to the unique readable magnetic signature.

5. The document of claim 2 wherein the digital watermark carries data that is related to other data on the document, and enables authentication of the document by comparison of the data in the digital watermark with other data on the document.

6. The document of claim 5 wherein the data related to the other data on the document is encrypted with respect to other data on the document.

7. A method of providing security to an identification document having at least one storage element capable of storing information, comprising:

providing an encryption key, the encryption key comprising a public key and a private key;

creating an optically variable device (OVD) in a machine readable format, the OVD associated with the public key;

generating a payload of data for storage in the storage element;

encrypting at least a portion of the payload of data with the private key; and

transmitting the encrypted payload of data to at least one location on the identification document.

8. The method of claim 7, wherein generating a payload of data further comprises basing at least a portion of the data payload on data that is randomly selected from data stored in the storage element.

9. The method of claim 7, wherein generating a payload of data further comprises basing at least a portion of the data payload on data that is encrypted from data that is stored in the storage element.

10. The method of claim 7, wherein the storage element comprises at least one of an optically variable device (OVD), optical storage media, hologram, KINEGRAM, Exelgram, Pixelgram, three dimensional bar code, a two dimensional bar code, a magnetic stripe, and a chip.

11. The method of claim 7, wherein transmitting the encrypted payload comprises at least one of embedding, digitally watermarking, printing, and encoding encrypted data in at least one location on the identification document.

12. An identification document comprising:

an OVD with embedded machine readable data;

a substrate with one or more structures carrying data that is associated with the machine readable data embedded in the OVD.

13. The document of claim 12 wherein the OVD comprises an embossed hologram with an embedded digital watermark.

14. The document of claim 13 wherein the digital watermark carries an issuer identifier.

15. The document of claim 13 wherein the digital watermark carries data that is related to other data on the document, and enables authentication of the document by comparison of the data in the digital watermark with other data on the document.

16. A method of verifying a document comprising:

determining jurisdictional information related to the document, wherein the jurisdictional information is mathematically related to a digital watermark embedded in the document; and

using the jurisdictional information to extract the digital watermark embedded in the document.

17. A method of verifying a document comprising:

extracting a public key from a machine readable feature on the document;

extracting a message payload from another machine readable feature on the document, the message payload being encrypted by a private key that forms part of a public-private key pair with the public key; and

using the public key to de-scramble the message payload.

18. The method of claim 17 wherein at least one of the machine readable features comprises an optically variable device.

19. The method of claim 17 wherein at least one of the machine readable features comprises a digital watermark.

20. The method of claim 17 wherein the message payload comprises a digital watermark message payload, and the public key is stored in a machine readable optically variable device.

21. A method of verifying a document comprising:

determining jurisdictional information related to the document, wherein the jurisdictional information is used to obtain a watermark key which is related to a digital watermark embedded in the document; and

using the key to extract the digital watermark embedded in the document.

22. The method of claim 21, wherein the document comprises a machine-readable feature, which carries the jurisdictional information, and wherein said determining step comprises reading the machine-readable feature.

23. The method of claim 21, wherein the jurisdictional information comprises an index, which is used to interrogate a database to obtain the watermarking key.

24. The method of claim 21, wherein the jurisdictional information is combined with predetermined data to form the watermarking key.

25. The method of claim 21, wherein the jurisdictional information comprises the watermarking key.

26. The method of claim 22, wherein the jurisdictional information comprises the watermarking key.

27. The method of claim 21, wherein the jurisdictional information is mathematically related to the digital watermark through a cryptographic relationship.

28. The method of claim 21, wherein the jurisdictional information is mathematically related to the digital watermark through a watermarking key.